SIEMENS

SIMATIC iMap under Windows XP SP2 - Overview 1

Changing the settings 2

Literature 3

SIMATIC

Component Based Automation SIMATIC iMap - Settings under Windows XP SP2

User Manual (Compact)

Edition 09/2004
A5E00352920-01

Safety Guidelines

This manual contains notices which you should observe to ensure your own personal safety as well as to avoid property damage. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring to property damage only have no safety alert symbol.

Danger

indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.

Warning

indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

Caution

used with the safety alert symbol indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

Caution

used without safety alert symbol indicates a potentially hazardous situation which, if not avoided, may result in property damage.

Notice

used without the safety alert symbol indicates a potential situation which, if not avoided, may result in an undesirable result or state.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The device/system may only be set up and operated in conjunction with this documentation. Only qualified personnel should be allowed to install and work on the equipment. Qualified persons are defined as persons who are authorized to commission, to earth, and to tag circuits, equipment and systems in accordance with established safety practices and standards.

Intended Use

Please note the following:

Warning

This device and its components may only be used for the applications described in the catalog or technical description, and only in connection with devices or components from other manufacturers approved or recommended by Siemens.

This product can only function correctly and safely if it is transported, stored, set up and installed correctly, and operated and maintained as recommended.

Trademarks

All designations marked with ® are registered trademarks of Siemens AG. Other designations in this documentation might be trademarks which, if used by third parties for their purposes, might infringe upon the rights of the proprietors.

Copyright Siemens AG, 2004. All rights reserved
Reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Disclaimer of Liability
We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in the manual are reviewed regularly, and any necessary corrections will be included in subsequent editions. Suggestions for improvement are welcomed.

Siemens AG
Automation and Drives Group
P.O. Box 4848, D-90327 Nuremberg (Germany)

Siemens AG 2004
Technical data subject to change

Table of contents

1 SIMATIC iMap under Windows XP SP2 - Overview 1-1

2 Changing the settings 2-1

2.1 Changing the firewall settings 2-1

2.2 Changing the DCOM access permissions 2-8

2.3 Reversing your changes 2-11

3 Literature 3-1

SIMATIC iMap under Windows XP SP2 - Overview

1

Introduction

Windows XP service pack 2 (Windows XP SP2) contains additional security functions that have to be adapted before they can be used with SIMATIC iMap.

The most important changes are the following:

- The firewall is activated for all LAN connections.
- Unauthenticated DCOM access is prevented.

Effects on SIMATIC iMap

The above security functions have the following effects when SIMATIC iMap V2.0 or 2.0 SP1 is used in online mode:

- Online connections cannot be established fully from SIMATIC iMap to the target devices in the plant.
- The online and diagnostic functions cannot be used and interconnections cannot be downloaded in SIMATIC iMap.

Note

Communication between the PROFINET devices (PLC-PLC communication) is not affected by using Windows XP SP2 on the engineering PC/PG.

Remedy: Temporarily change the operating system settings

If you have installed Windows XP SP2 on the engineering PG/PC with SIMATIC iMap, you will have to temporarily change the operating system settings to meet the SIMATIC iMap requirements for the duration of the plant testing and start-up phase.

Caution

Some of the security functions are reset to the previous Windows XP security level (pre-SP2) for the duration of the change.

Recommendation: To guarantee that your PG/PC is protected against viruses and unauthorized access, you should reverse the changes to the security functions when the testing and start-up phase is complete.

Steps required to change the settings

1. Change the firewall settings
   - Allow external access to the SIMATIC iMap application
   - Set up port for DCOM access
2. Change DCOM access permissions for communication between SIMATIC iMap and the PROFINET devices.

The procedure for changing and restoring the settings is described below.

Saving the original settings

The following sections require the Windows XP SP2 default settings. These are shown in the graphics. The "Reversing your changes" section describes how to restore these Windows XP SP2 default settings.

To be able to restore the original status, you must save your computer's current settings (e.g. in the form of screen shots) before you make any changes. This is particularly important if the settings on your PG/PC differ from the default settings.

See also

Changing the firewall settings (Page 2-1)

Changing the DCOM access permissions (Page 2-8)

Reversing your changes (Page 2-11)

Changing the settings

2

2.1 Changing the firewall settings

You will have to temporarily change the firewall settings on your PG/PC in order to diagnose and test the plant using SIMATIC iMAP:

- Allow external access to the SIMATIC iMap application
- Set up port for DCOM access

Requirements

You will need administrator rights on the PG/PC in order to change the security functions.

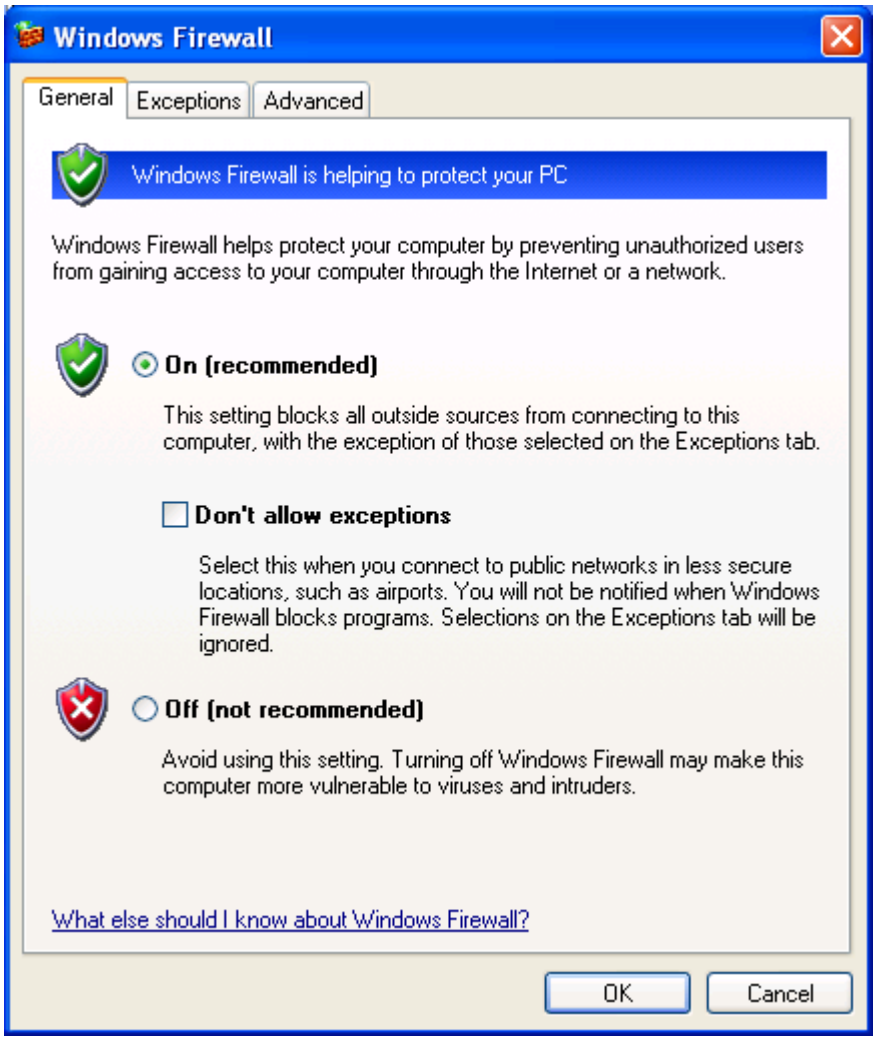
Discuss the changes with your network administrators or network operators if necessary.

Make sure that changes to the settings will not affect other installed applications.

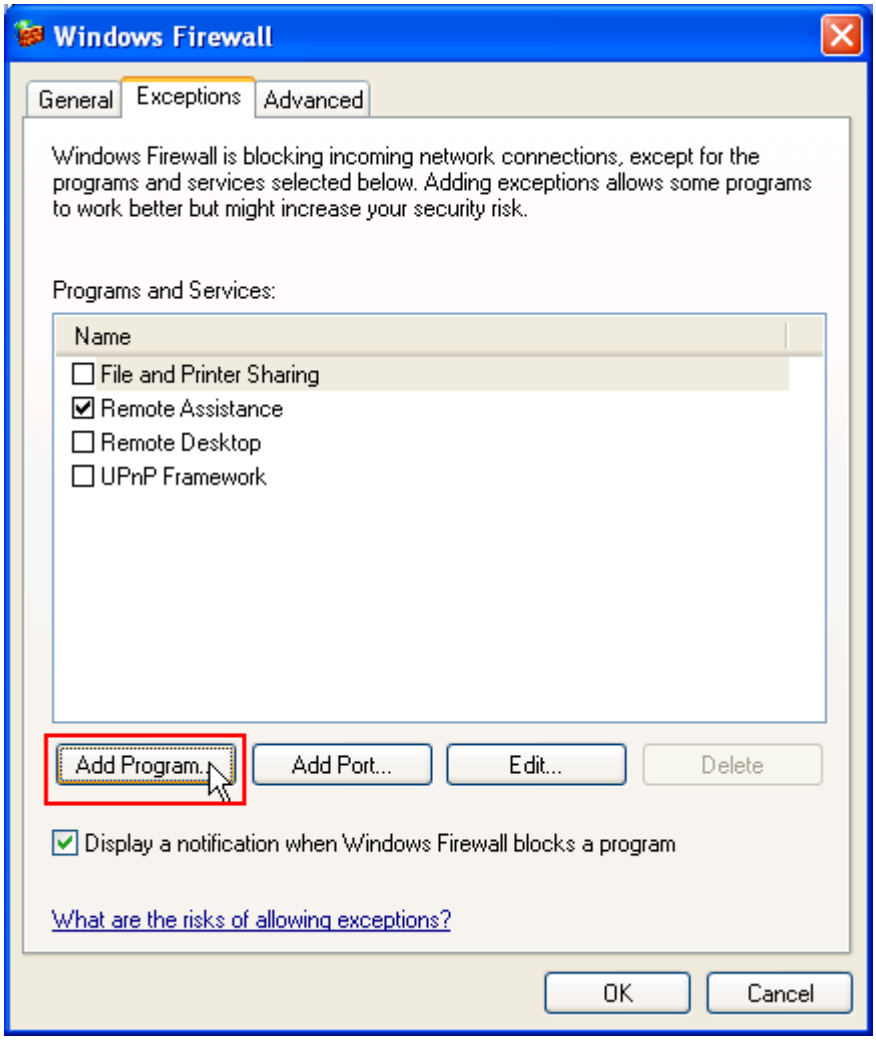
Change the firewall settings as follows:

1. Open the firewall from the Windows taskbar using the following command: **Start > Control Panel > Windows Firewall**.

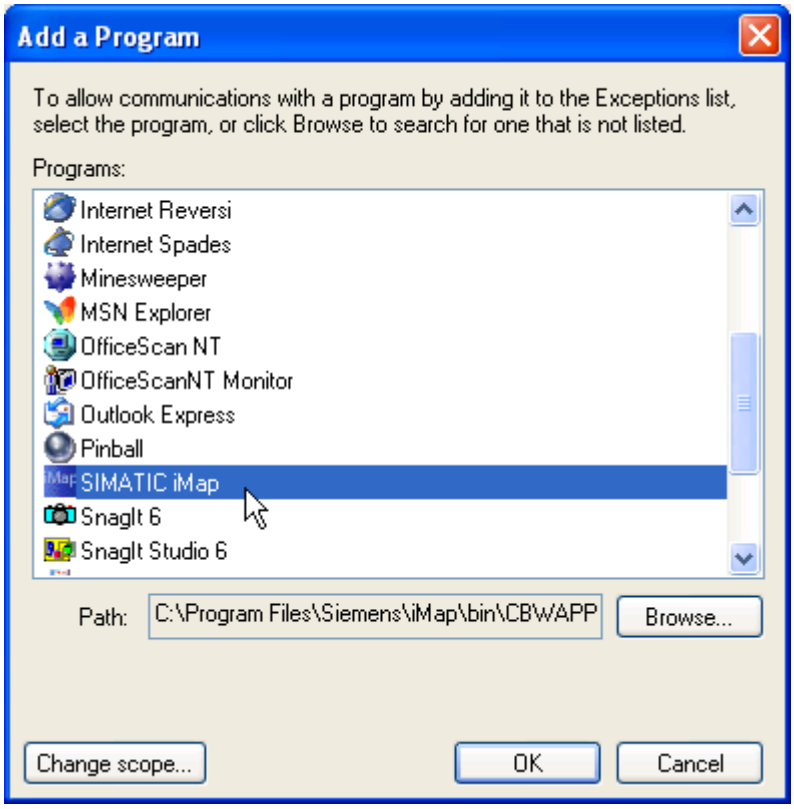
   The Windows Firewall dialog opens.


Windows Firewall
General
Exceptions
Advanced
Windows Firewall is helping to protect your PC
Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
What else should I know about Windows Firewall?
OK
Cancel

2. Select the "Exceptions" tab and click on the "Add Program" button to allow external access to the SIMATIC iMap application.



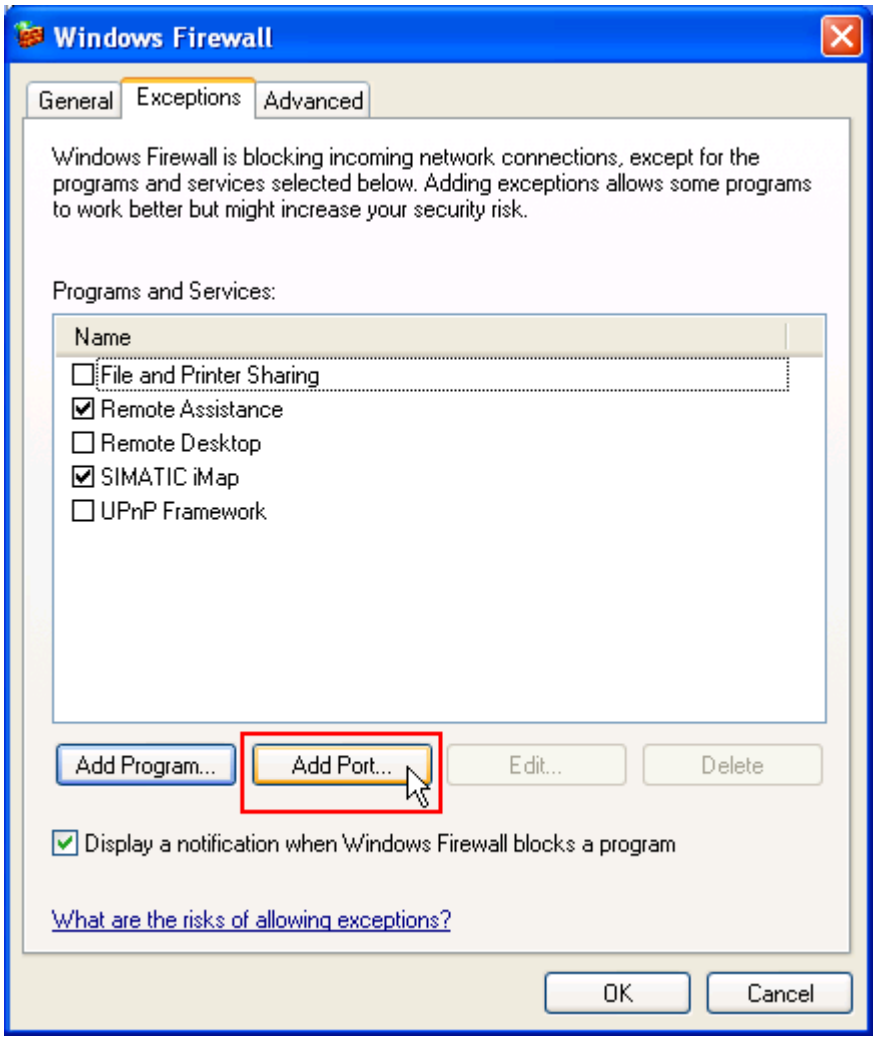
3. Select "SIMATIC iMap" from the "Programs:" box. Click on the "Browse ..." button if necessary.



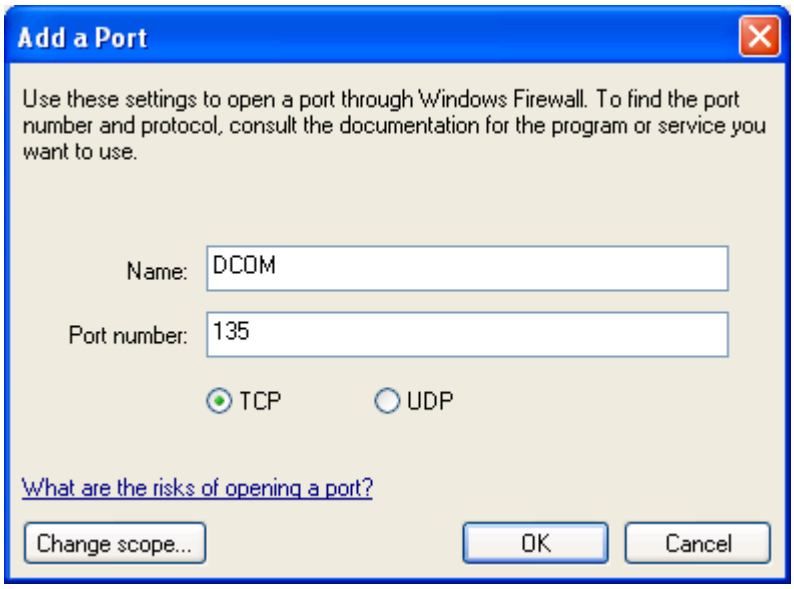
4. Confirm your selection with OK.

   Result: SIMATIC iMap is added to the list of exceptions. This means that external DCOM access to SIMATIC iMap is now possible.

5. On the "Exceptions" tab, click on the "Add Port" button to set up a port for DCOM access.



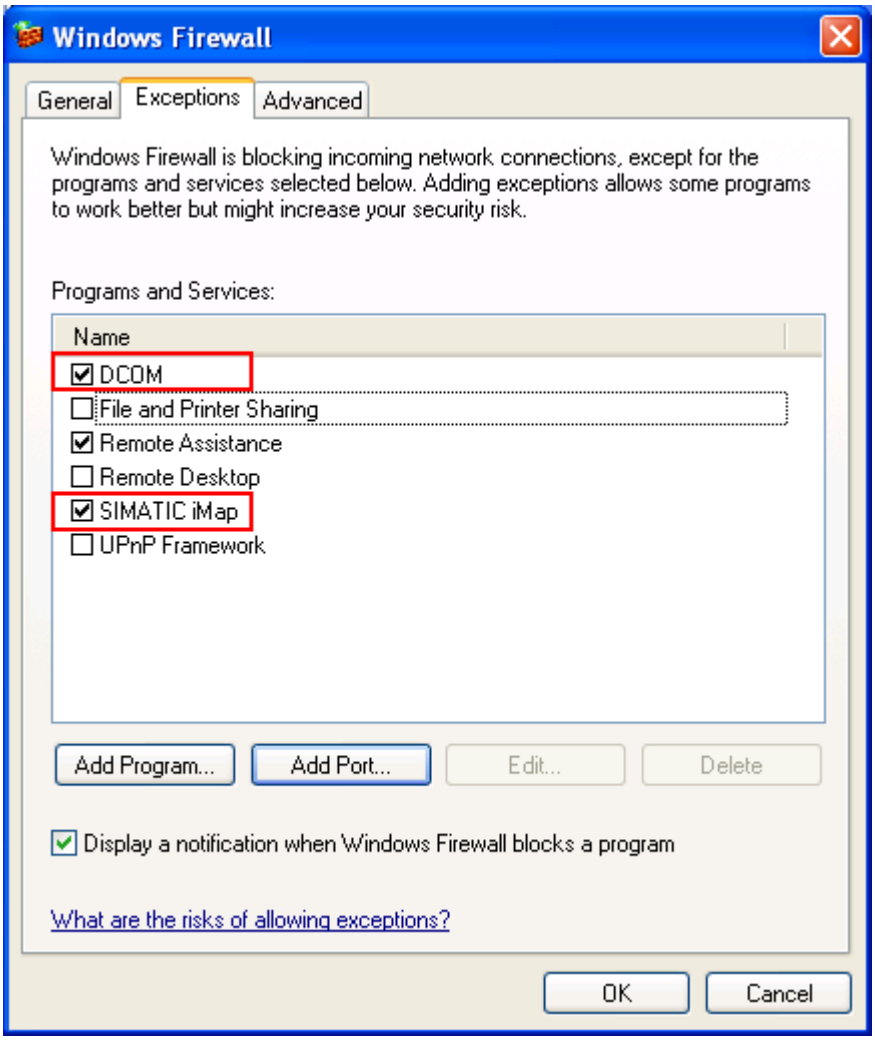
6. Enter the following in the "Add a Port" dialog:
   - the name "DCOM"
   - the port number 135
   - and select the "TCP" option.


Add a Port
Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.
Name:
DCOM
Port number:
135
TCP
UDP
What are the risks of opening a port?
Change scope...
OK
Cancel

7. Click on OK to confirm your input.

   Result: DCOM port 135 is added to the list of firewall exceptions.

The following screenshot shows the new settings in the firewall exceptions.



8. Click on OK to confirm your input.

This completes the firewall settings.

Caution

External DCOM access to the computer is now possible once more.

See also

Reversing your changes (Page 2-11)

2.2 Changing the DCOM access permissions

The DCOM access rights have to be temporarily reset to WinXP SP1 level to allow communication between PROFINET devices and SIMATIC iMap.

Requirements

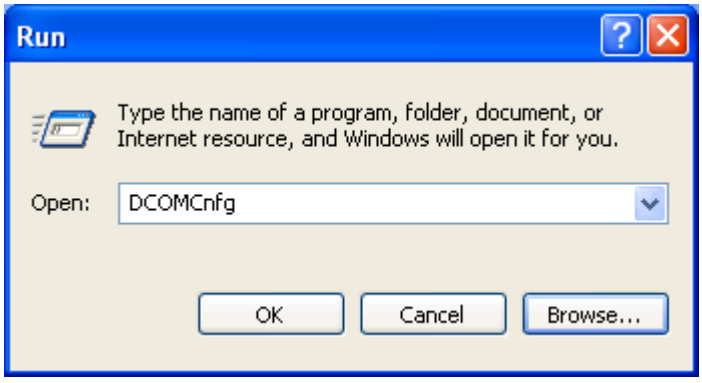
You will need administrator rights on the PG/PC in order to change the security functions.

Discuss the changes with your network administrators or network operators if necessary.

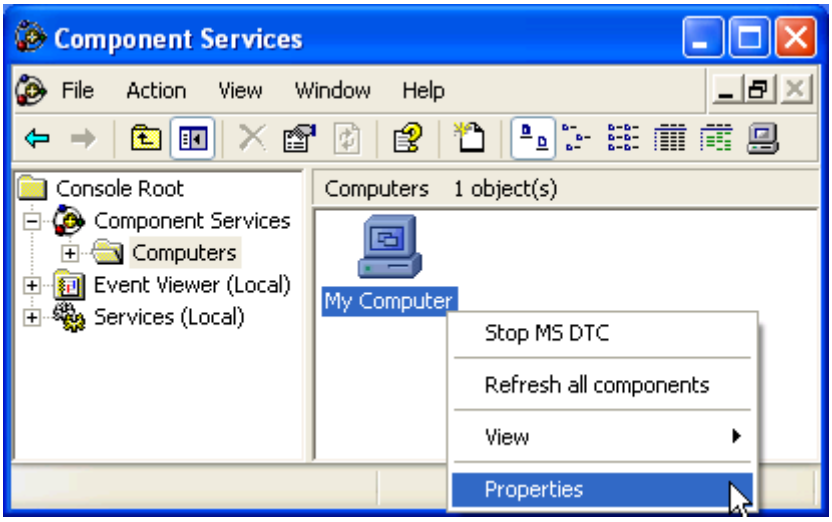
Make sure that changes to the settings will not affect other installed applications.

Set the DCOM access permissions as follows:

1. Select **Start > Run...** from the Windows taskbar, enter "DCOMCnfg" and click on OK to confirm:

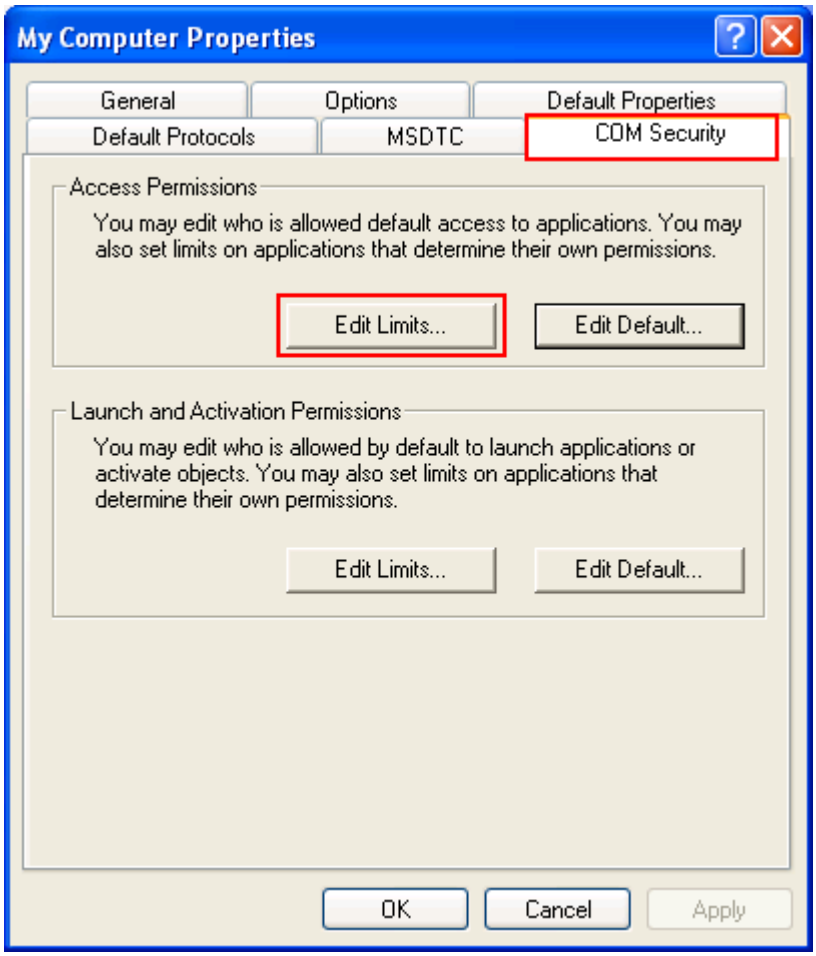


2. In the "Component Services" dialog
   - open the "Console Root\Component Services\Computers" folder,
   - select the "My Computer" icon from the "Computers" window and
   - select "Properties" from the context menu (right mouse button).

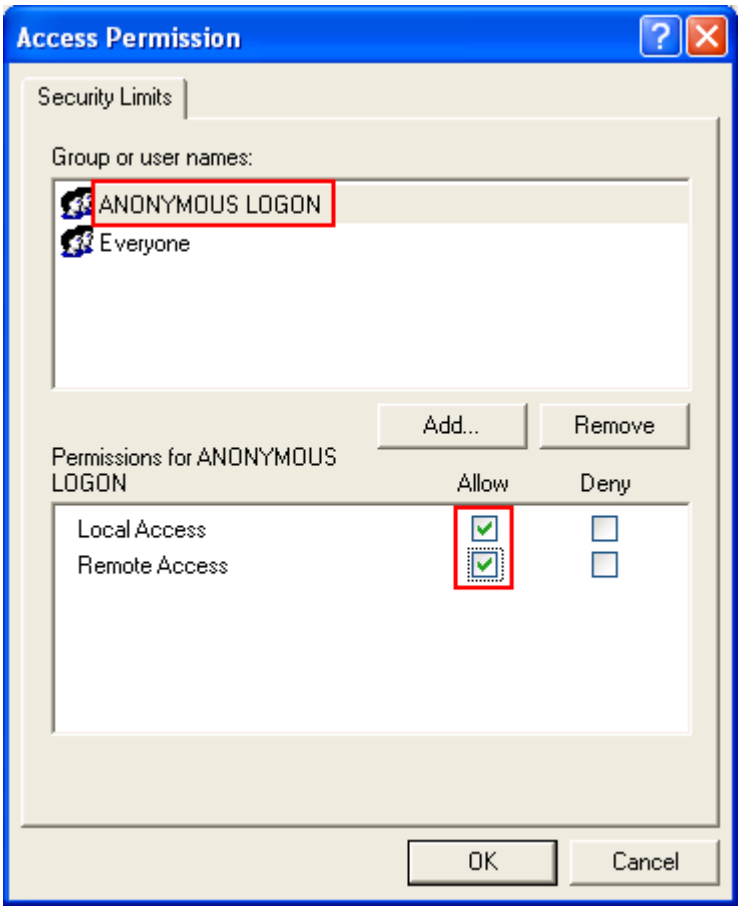


The "My Computer Properties" dialog opens.

3. Select the "COM Security" tab, then click on the "Edit Limits..." button.


My Computer Properties
General
Options
Default Properties
Default Protocols
MSDTC
COM Security
Access Permissions
You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.
Edit Limits...
Edit Default...
Launch and Activation Permissions
You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.
Edit Limits...
Edit Default...
OK
Cancel
Apply

4. In the "Access Permission" dialog, select the "ANONYMOUS LOGON" entry and check the "Allow" check boxes for both "Local Access" and "Remote Access".



5. Click on OK to confirm your input.

Result: This completes the changes to the DCOM access permissions.

Caution

This resets the WinXP SP2 security level to SP1 level.

The default setting for Windows XP SP2 only permits local access for "ANONYMOUS LOGON" (see also the "Reversing your changes" section).

See also

Reversing your changes (Page 2-11)

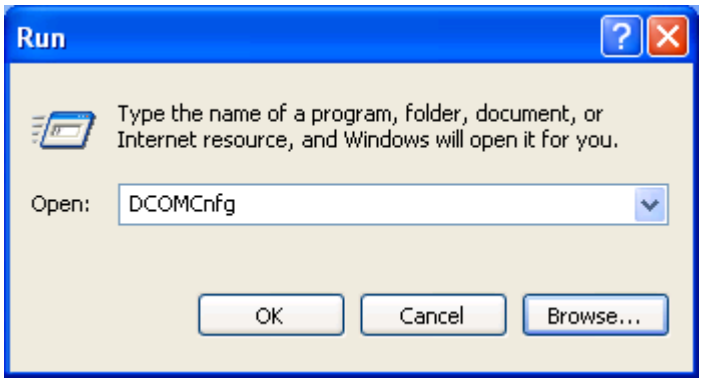
2.3 Reversing your changes

The changed security functions for the Windows XP SP2 operating system can be restored as required. To do this, you must reverse the changes you have made:

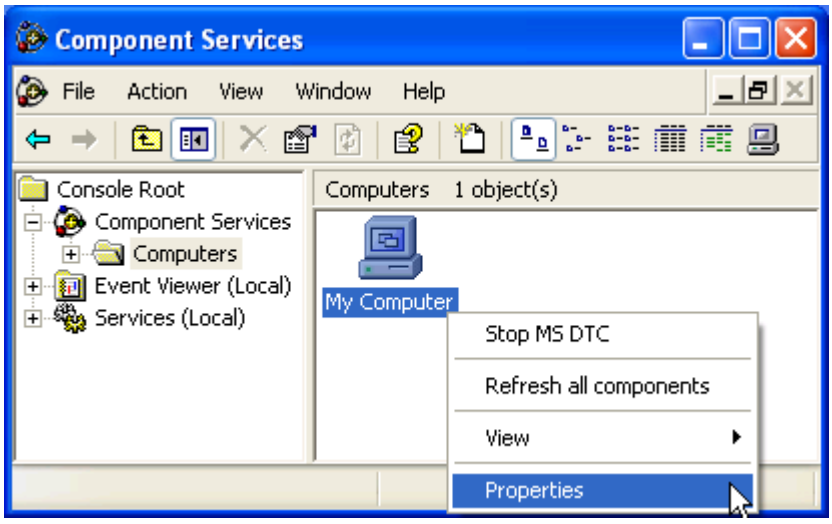
- Change the DCOM access permissions - so that you reset the DCOM access permissions to the WinXP SP2 level.
- Change the firewall settings - so that you deactivate or remove the exceptions that you added.

Undo the change to the DCOM access permissions as follows

1. Open the Component Services for your computer by selecting **Start > Run...** from the Windows taskbar, entering "DCOMCnfg" and clicking on OK to confirm:

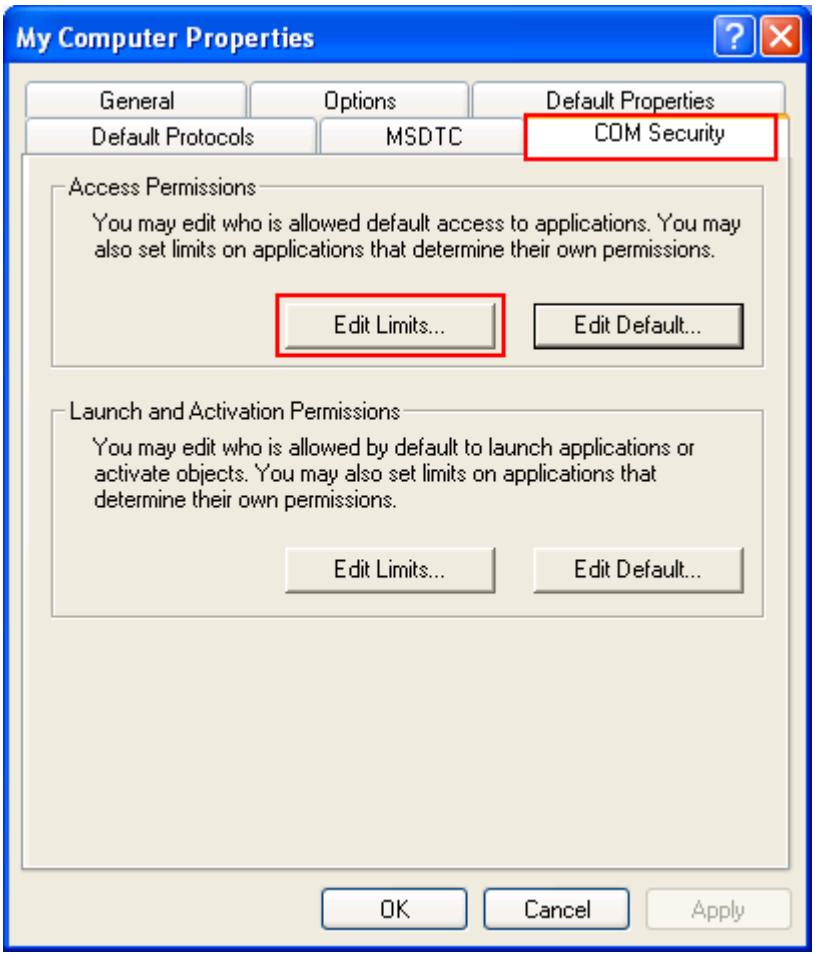


2. In the "Component Services" dialog
   - open the "Console Root\Component Services\Computers" folder,
   - select the "My Computer" icon from the "Computers" window and
   - select "Properties" from the context menu (right mouse button).

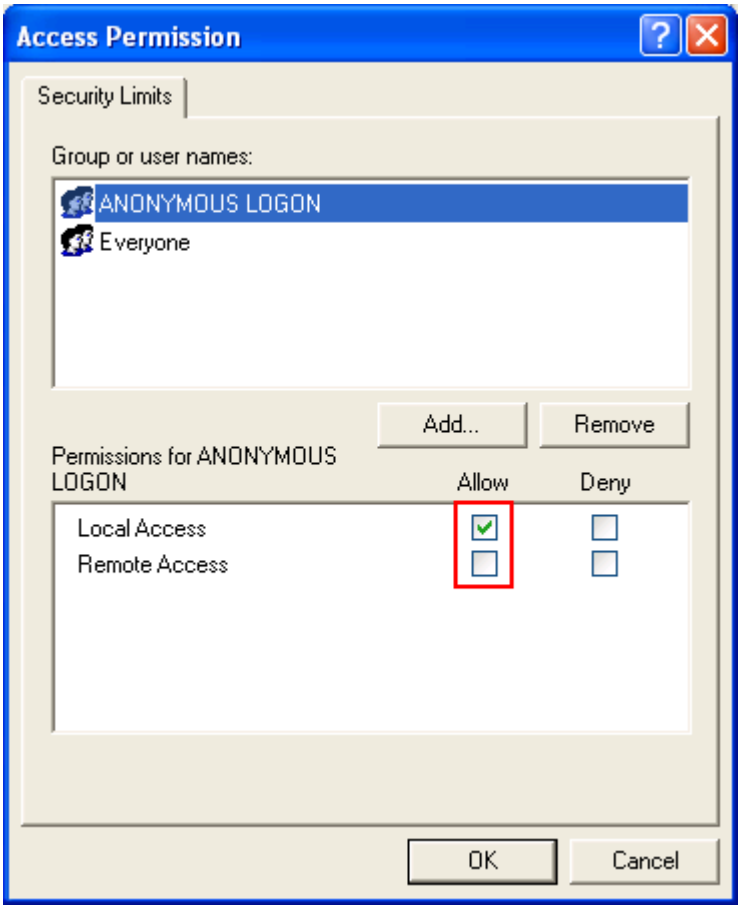


The "My Computer Properties" dialog opens.

3. Select the "COM Security" tab, then click on the "Edit Limits..." button.


My Computer Properties
General
Options
Default Properties
Default Protocols
MSDTC
COM Security
Access Permissions
You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.
Edit Limits...
Edit Default...
Launch and Activation Permissions
You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.
Edit Limits...
Edit Default...
OK
Cancel
Apply

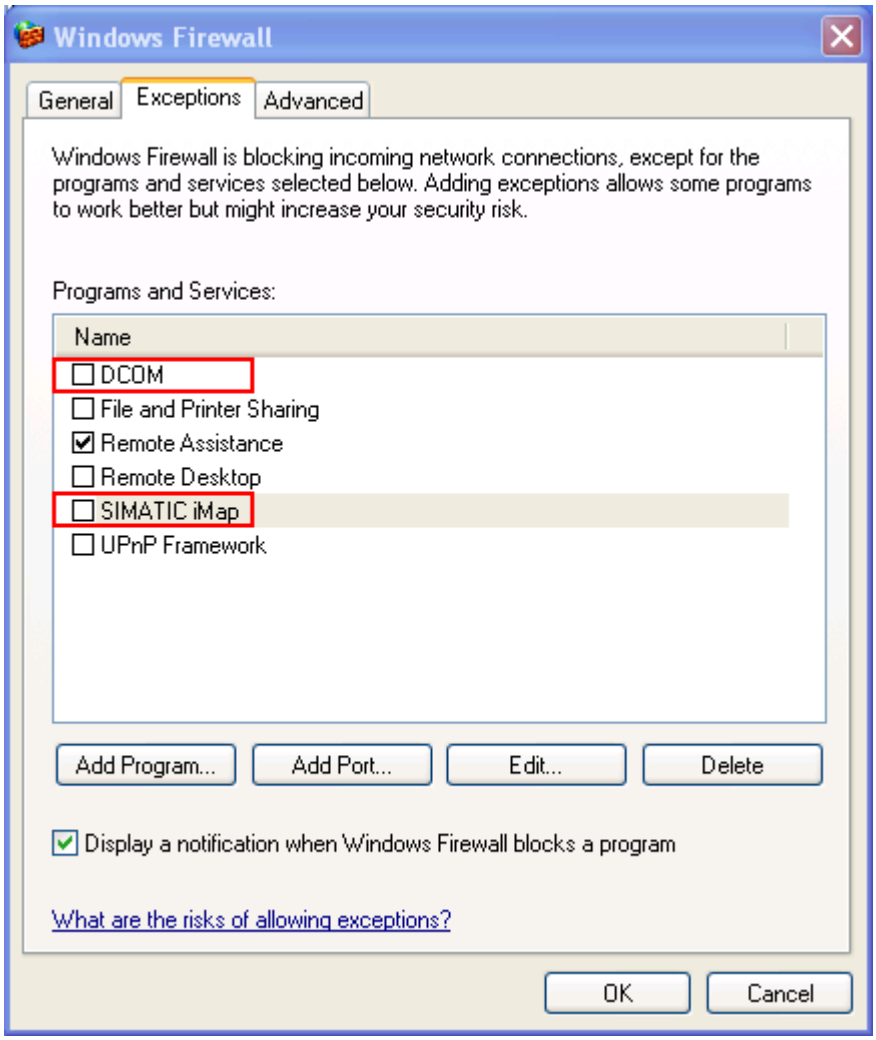
4. In the "Access Permission" dialog, restore the permissions to their original status by selecting the "ANONYMOUS LOGON" entry and deactivating the "Remote Access" option. This is the default setting for Windows XP SP2.



5. Click on OK to confirm the change.

Undo your changes to the firewall settings as follows

1. Open the firewall from the Windows taskbar using the following command: **Start > Control Panel > Windows Firewall**.
2. Select the "Exceptions" tab and uncheck the check boxes for the added exceptions - "SIMATIC iMap" and "DCOM" (port 135).



3. Click on OK to confirm the change.

This reverses the changes you made to the firewall settings, i.e. restores the Windows XP SP2 security functions.

Note

If necessary, you can remove the added exceptions "SIMATIC iMap" and "DCOM" (port 135) from the "Exceptions" tab altogether. However, it is sufficient just to uncheck the check boxes. This means that you can quickly reactivate the settings if you need to.

See also

Changing the firewall settings (Page 2-1)

Changing the DCOM access permissions (Page 2-8)

Literature

3

Further information on Windows XP SP2

can be found in:

- Windows XP Service Pack 2 Overview
  http://msdn.microsoft.com/security
- Windows XP Service Pack 2 - Security Information for Developers
  http://msdn.microsoft.com/security/productinfo/XPSP2/default.aspx
- Changes to Functionality in Microsoft Windows XP Service Pack 2
  http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx